REMARKS

Claims 1-9, 12-17, 19-21, 23, 25-41, and 45-47 are currently pending in the subject application and are presently under consideration. Claims 1, 12, 16, 17, 25, 30, 31, 38, 39, and 41 have been amended as shown on pages 2 to 9 of the Reply. Applicants' representative appreciates the Examiner's indication of allowable subject matter in claims 24-29. The amendments presented herein attempt to embody the indicated allowable matter in the remaining independent claims. Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claims 1-9, 12-17, 19-21, 23, 30-41, and 45-47 Under 35 U.S.C. §102(b)

Claims 1-9, 12-17, 19-21, 23, 30-41, and 45-47 stand rejected under 35 U.S.C. §102(b) as being allegedly anticipated by Swiler, *et al.* (US 7,013,395). It is respectfully requested that this rejection be withdrawn for at least the following reasons. Swiler, *et al.* fails to disclose or suggest each and every element recited in the subject claims.

> A single prior art reference anticipates a patent claim only if it expressly or inherently describes ***each and every limitation set forth in the patent claim***. *Trintec Industries, Inc. v. Top-U.S.A. Corp.,* 295 F.3d 1292, 63 USPQ2d 1597 (Fed. Cir. 2002); *See Verdegaal Bros. v. Union Oil Co. of California,* 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

The subject matter as claimed generally relates to generating a set of security guidelines, security data, and/or security components for industrial controllers in an industrial automation environment. In particular, input can be received in the form of an abstract description or model of a factory, where the factory description can include information regarding the industrial controllers. The generated security data can include a set of recommended security components, related interconnection topology, connection configurations, application procedures, security policies, rules, user procedures, and/or user practices related to the industrial controllers. Additionally, based on generated data, measures can be taken to improve security in the automation environment, such as automatic security component installation. Also, security in the automation environment can be verified against industry standards, such as one or more international organization for standardization (ISO) standards in one example. To this end, claim

1 as amended recites, in part, ***a validation component that . . . automatically installs one or more security components in response to the one or more vulnerabilities***. Swiler, *et al.* fails to disclose such claimed aspects.

Swiler, *et al.* generally relates to a tool that analyzes computer systems for related security attributes. (*See*, Abstract). In particular, Swiler, *et al.* appears to contemplate generating an attack graph based at least in part on inputs including attack templates, configuration files, and attacker profiles. Swiler, *et al.* generally contemplates security analysis for computers, such as "workstations, servers, or routers." (*See e.g.*, column 4, lines 48-52), and creates the attack graph upon request. Swiler, *et al.*, however, fails to disclose or suggest ***a component that automatically installs one or more security components in response to the one or more vulnerabilities***, as recited in claim 1.

On the contrary, Swiler, *et al.* generates the attack graph to show possible insufficiencies in security of a computer network. Swiler, *et al.*, however, is completely silent regarding performing automated install of security components as recited in claim 1. In particular, the Examiner has indicated similar subject matter in former claim 24 allowable over Swiler, *et al.* (*See*, page 35 of the Final Office Action dated January 2, 2009). Thus, claim 1 is amended herein to include this matter and overcomes rejection in view of Swiler, *et al.* for at least this reason.

Moreover, claim 12 has been amended to recite similar aspects, namely ***automatically installing one or more security components based at least in part on the one or more security outputs***. For at least this reason, rejection of claim 12 should be withdrawn. Claim 17 is also amended to incorporate the allowable aspect of former claim 24 – ***a component to automatically install one or more security components in response to detected security problems***. Accordingly, rejection of this claim should be withdrawn. Additionally, claim 31 is amended to similarly recite, in part, ***wherein the security event includes automatically installing one or more security components***. Thus, rejection of this claim should be withdrawn as well.

Claim 30, as amended, additionally recites subject matter that the Examiner has indicated as allowable with respect to claim 26. Namely, claim 30 recites in part ***determining whether the automated security validation system conforms to one or more industry standards*** *based on at least one of the security assessments, security compliance checks, and security vulnerability scanning*. Swiler, *et al.* fails to disclose or suggest such aspects. In particular, it seems the

Examiner's indicated allowability of claim 26 in view of this aspect added in reply to the previous Office Action. Thus, rejection of this claim should be withdrawn. Claim 39 has been similarly amended to recite *generating an alarm where a current data pattern is* ***determined to be outside of a predetermined threshold associated with one or more industry standards***. Swiler, *et al.* fails to disclose or suggest such aspects for at least the reasons provided above, and accordingly, rejection of claim 39 should be withdrawn. In addition, claim 41 is amended herein to recite *means for generating a security event where the access patterns are determined to be out of tolerance from stored access patterns* ***as compared to one or more industry standards***. As shown, Swiler, *et al.* fails to disclose or suggest such aspects; accordingly, rejection of this claim should be withdrawn.

Independent claim 16 has been amended to recite *means for* ***automatically detecting a deviation from the at least one access pattern*** *and means for* ***performing an automated action based at least in part on the detected deviation***. Swiler, *et al.* additionally fails to disclose or suggest these aspects. The Examiner broadly asserts that Swiler, *et al.* teaches learning access patterns by stating that claim 16 is rejected for the same reasons as claim 1; however, the recited aspects are not identical to those recited in claim 1. Swiler, *et al.* does not contemplate learning access patterns; though Swiler, *et al.* appears to claim polling computers in a dependent claim, this is not indicative of learning access patterns thereof. In addition, Swiler, *et al.* is completely silent regarding ***automatically detecting a deviation from the at least one access pattern*** and ***performing an automated action based at least in part on the detected deviation***, as recited in claim 16.

Further, the Examiner asserts that Swiler, *et al.* discloses learning/applying aspects of deviation pattern detection and automated remediation of the same in that a "user of the analysis tool can apply results obtained of potential/detected attack/vulnerabilities so as to mitigate said attack/vulnerabilities…." (*See*, page 34 of the Final Office Action). Claim 16, as amended however, recites automatically detecting the deviation from the access pattern. A user is not typically equipped to *automatically* detect such a deviation, much less perform an automated activity based on such. For at least these reasons, rejection of claim 16 should be withdrawn.

In view of at least the foregoing, it is readily apparent that Swiler, *et al.* fails to disclose or suggest each and every element recited in claims 1, 12, 16, 17, 30, 31, 39, and 41.

Accordingly, it is respectfully requested that rejection of these claims, as well as claims 2-9, 13-15, 19-21, 23, 32-38, 40, and 45-47, which depend therefrom, be withdrawn.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [ALBRP303USC].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,
AMIN, TUROCY & CALVIN, LLP

/David Matthew Noonan/
David Matthew Noonan
Reg. No. 59,451

AMIN, TUROCY & CALVIN, LLP
57TH Floor, Key Tower
127 Public Square
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731